CLAIM AMENDMENTS:

1. (Original) A system for detecting and deterring rollback attacks, comprising:

a variable time period (VTP);

a time duration to a next connection (TDNC);

an access log;

a server to transmit the variable time period (VTP) and the time duration to the next connection (TDNC) and to verify the access log; and

a client to update the access log approximately every variable time period (VTP) and to connect to the server approximately after the time duration to the next connection (TDNC).

2. (Original) The system as recited in claim 1, wherein the client is a personal computer (PC).

3. (Original) The system as recited in claim 1, wherein the client is a set-top box.

4. (Original) The system as recited in claim 1, wherein the server is a video home server.

5. (Original) The system as recited in claim 1, wherein the server is a pay-per-view video server.

6. (Original) The system as recited in claim 1, wherein the server is a video-on-demand server.

7. (Original) The system as recited in claim 1, wherein the server is a media content provider.

8. (Original) The system as recited in claim 1, wherein the next connection is a Secure Authenticated Channel (SAC).

9. (Original) The system as recited in claim 1, wherein the access log is used for billing.

10. (Original) A method for detecting and deterring rollback attacks, comprising:

establishing a shared secret between a client and a server;

transmitting, by the server to the client, a variable time period (VTP) and a time duration to a next connection (TDNC);

updating, by the client, an access log approximately every variable time period (VTP);

initiating, by the client to the server, a connection approximately after the time duration to the next connection (TDNC);

transmitting, by the client to the server, the access log; and

verifying, by the server, the access log.

11. (Original) The method as recited in claim 10, further comprising:

establishing a new shared secret between the client and the server each time the client connects to the server.

12. (Original) The method as recited in claim 10, further comprising:

establishing a new variable time period (VTP) and a new time duration to a next connection (TDNC) each time the client connects to the server.

13. (Original) The method as recited in claim 10, further comprising:

incrementing, by the client, a counter, after each update to the access log.

14. (Original) The method as recited in claim 10, further comprising:

automatically detecting an anomaly.

15. (Original) The method as recited in claim 14, further comprising:

decreasing the variable time period (VTP), upon detecting an anomaly.

16. (Original) The method as recited in claim 14, further comprising:

decreasing the time duration to a next connection (TDNC), upon detecting an anomaly.

17. (Original) The method as recited in claim 10, further comprising:

encrypting the access log.

18. (Original) The method as recited in claim 10, wherein each entry in the access log is encrypted.

19. (Original) The method as recited in claim 10, wherein the access log is re-created, each time the client connects to the server.

20. (Original) A machine for detecting and deterring rollback attacks, comprising:

a processor;

a storage device coupled to the processor;

a background component storable on the storage device and executable on the processor to update an access log approximately every variable time period (VTP); and

a content player component storable on the storage device and executable on the processor to update the access log to indicate content provided.

21. (Original) The machine recited in claim 20, wherein the background component is capable of encrypting the access log.

22. (Original) The machine recited in claim 20, wherein the background component is capable of encrypting each update to the access log.

23. (Original) The machine recited in claim 20, further comprising:

a communication component capable of connecting to a server approximately after a time duration to a next connection (TDNC).

24. (Original) The machine recited in claim 23, wherein the communication component is capable of transmitting the access log.

25. (Original) The machine recited in claim 23, wherein the communication component is capable of receiving a new variable time period (VTP) and a new time duration to the next connection (TDNC).

26. (Original) The machine recited in claim 20, wherein the communication component is capable of receiving a new access log.

27. (Original) The machine recited in claim 26, wherein the background component is capable of decrypting the new access log.

28. (Original) A machine-accessible medium having associated content capable of directing the machine to perform a method of detecting and deterring rollback attacks, the method comprising:

transmitting, by a server, a new access log; and

transmitting, by the server, a new variable time period (VTP) and a new time duration to the next connection (TDNC).

29. (Original) The machine-accessible medium as recited in claim 28, wherein the method further comprises:

receiving, by the server, an old access log; and

inspecting, by the server, the old access log.

30. (Original) The machine-accessible medium as recited in claim 28, wherein the method further comprises:

establishing, by the server, a shared secret with a client;

decrypting, by the server, the access log;

encrypting, by the server, the new access log; and

encrypting, by the server, the new variable time period (VTP) and the new time duration to the next connection (TDNC).

31. (Original) The machine-accessible medium as recited in claim 28, wherein the method further comprises:

initiating, by a client, a connection with the server;

transmitting, by the client, the access log to the server;

receiving, by the client, the new access log;

receiving, by the client, the new variable time period (VTP) and the new time duration to the next connection (TDNC); and

storing, by the client, the new access log, the new variable time period (VTP), and the new time duration to the next connection (TDNC).

32. (Original) The machine-accessible medium as recited in claim 28, wherein the method further comprises:

establishing, by a client, a shared secret with the server;

encrypting, by the client, the access log;

decrypting, by the client, the new access log; and

decrypting, by the client, the new variable time period (VTP) and the new time duration to the next connection (TDNC).

33. (Original) The machine-accessible medium as recited in claim 28, wherein the method further comprises:

updating, by a client, the new access log approximately every new variable time period (VTP).